SPYWOLF

Security Audit Report

Completed on

June 16, 2022

MADE IN USA 🇺🇸

OVERVIEW

This audit has been prepared for **Doge Kart** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

DOGE KART

PROJECT DESCRIPTION

According to their whitepaper:

Release Date: June 16, 2021

Category:

CONTRACT INFO

Token Name
DogeKart Token

Symbol
KART

Contract Address
0xA406C4f80fc26F0926F5f53c91E3740260258249

Network
Binance Smart Chain

Language
Solidity

Deployment Date
June 16, 2022

Verified?
Yes

Total Supply
1,000,000,000

Status
Launched

TAXES

Buy Tax
14%

Sell Tax
14%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of June 16, 2022)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxSellTxAmount	No additional Info
10,000,000	

LP Address(es)

Liquidity not added yet

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	1000000000 KART
Median Transfer Amount	1000000000 KART
Average Transfer Amount	1000000000 KART
First transfer date	2022-06-16
Last transfer date	2022-06-16
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2022-06-16 06:48:12 UTC
Created	2022-06-16 06:48:12 UTC
Create TX	0xca9bbcb55dd663a62d971166e0b3743dcc2b83737e3403e583df13acab9c6e7b
Creator	0x6821343d926c204be7bea0803c001b9c654632ef

FEATURED WALLETS

Owner address	0x6821343d926c204BE7BEA0803c001b9C654632Ef
Buyback wallet	0x340463a124bb850bf3346b5ac9a09388fc0c6335
Charity wallet	0x425CE2490116c64f854E1bA56EaE98724D733916
Marketing wallet	0x23Ec94682A0Bf16318518536646b38f70De35559
LP address	**No liquidity added yet**

TOP 3 UNLOCKED WALLETS

1

100% Same as owner

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Owner can mint (create) new tokens and sell them in market at any time. This can lead to drastic token price inflation (-99%).

```
function burn(address account, uint256 amount) onlyOwner public virtual {
    require(account != address(0), "ERC20: burn to the zero address");
    _tTotal += amount;
    _tOwned[account] += amount;
    emit Transfer(address(0), account, amount);
}
```

Owner can change cashier and antiSnipe contracts to any contract and functionalities may not correspond to the function's names.

```
function setInitializers(address aInitializer, address cInitializer) external onlyOwner {
    require(cInitializer != address(this) &&
    aInitializer != address(this) && cInitializer != aInitializer);
    reflector = Cashier(cInitializer);
    antiSnipe = AntiSnipe(aInitializer);
}
```

Adding initial liquidity and transfers fail, because the owner() returns _renounced, which is set to 0x0 address.
The return of function owner() must be changed to _owner instead of _renounced.

```
function owner() public view returns (address) {
    return _renounced;
}
```

FOUND THREATS

⚠ High Risk

Owner can restrict address from trading via antiSnipe interface, which can be changed in future.
Owner can blacklist address from trading, making it impossible to sell.
Owner can change cooldown time between trades, making it impossible to sell.
Owner can set gas limits for each transaction, making it impossible to sell on network congestion if limits are set too low.

```
function setBlacklistEnabled(address account, uint256 time) external onlyOwner {
    antiSnipe.setBlacklistEnabled(account, time);
}
function setBlacklistEnabledMultiple(address[] memory accounts, uint256 time) external onlyOwner {
    antiSnipe.setBlacklistEnabledMultiple(accounts, time);

function setBuyCooldown(uint256 time) external onlyOwner {
    antiSnipe.setBuyCooldown(time);
}
function setProtectionSettings(bool _antiSnipe, bool _antiGas,
bool _antiBlock, bool _cooldown, bool _antiSpecial) external onlyOwner() {
    antiSnipe.setProtections(_antiSnipe, _antiGas, _antiBlock, _cooldown, _antiSpecial);
}
function setGasPriceLimit(uint256 gas) external onlyOwner {
    require(gas >= 75, "Too low.");
    antiSnipe.setGasPriceLimit(gas);
}
```

FOUND THREATS

⚠ Medium Risk

Owner can set buy/sell/transfer fees up to 25%.
Combined buy+sell=50%.

```
StaticValuesStruct public staticVals = StaticValuesStruct({
    maxBuyTaxes: 2500,
    maxSellTaxes: 2500,
    maxTransferTaxes: 2500,
    masterTaxDivisor: 10000
    });

function setTaxes(uint16 buyFee, uint16 sellFee, uint16 transferFee) external onlyOwner {
    require(buyFee <= staticVals.maxBuyTaxes
            && sellFee <= staticVals.maxSellTaxes
            && transferFee <= staticVals.maxTransferTaxes);
    _taxRates.buyFee = buyFee;
    _taxRates.sellFee = sellFee;
    _taxRates.transferFee = transferFee;
}
```

- Recommendation:
  - Good taxes practice is buy and sell fees combined not to exceed 25%.

⚠ Low Risk

Owner can change max transaction and wallet limit, but can't set it lower than 0.1% of total supply.

```
function setMaxTxPercent(uint256 percentBuy, uint256 divisorBuy,
uint256 percentSell, uint256 divisorSell) public onlyOwner {
require((_tTotal * percentBuy) / divisorBuy >= (_tTotal / 1000)
        && (_tTotal * percentSell) / divisorSell >= (_tTotal / 1000),
        "Max Transaction amt must be above 0.1% of total supply.");
_maxTxBuyAmount = (_tTotal * percentBuy) / divisorBuy;
_maxTxSellAmount = (_tTotal * percentSell) / divisorSell;
_limits.maxTxBuyAmtUI = (startingSupply * percentBuy) / divisorBuy;
_limits.maxTxSellAmtUI = (startingSupply * percentSell) / divisorSell;
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

DOGE KART

GOOD PRACTICES FOUND

- ✔ The owner cannot stop or pause the contract
- ✔ The owner can set a transaction limit, but can’t lower it than 0.1% of total supply

*There is no information about tokens distribution in the project's whitepaper and/or website:

TOKENOMICS

THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ KYC Failed

KYC was failed after SpyWolf analysis

WEBSITE

Website URL
https://dogekart.io/

Domain Registry
Sarek Oy

Domain Expiration
Expires on 2023-05-28

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

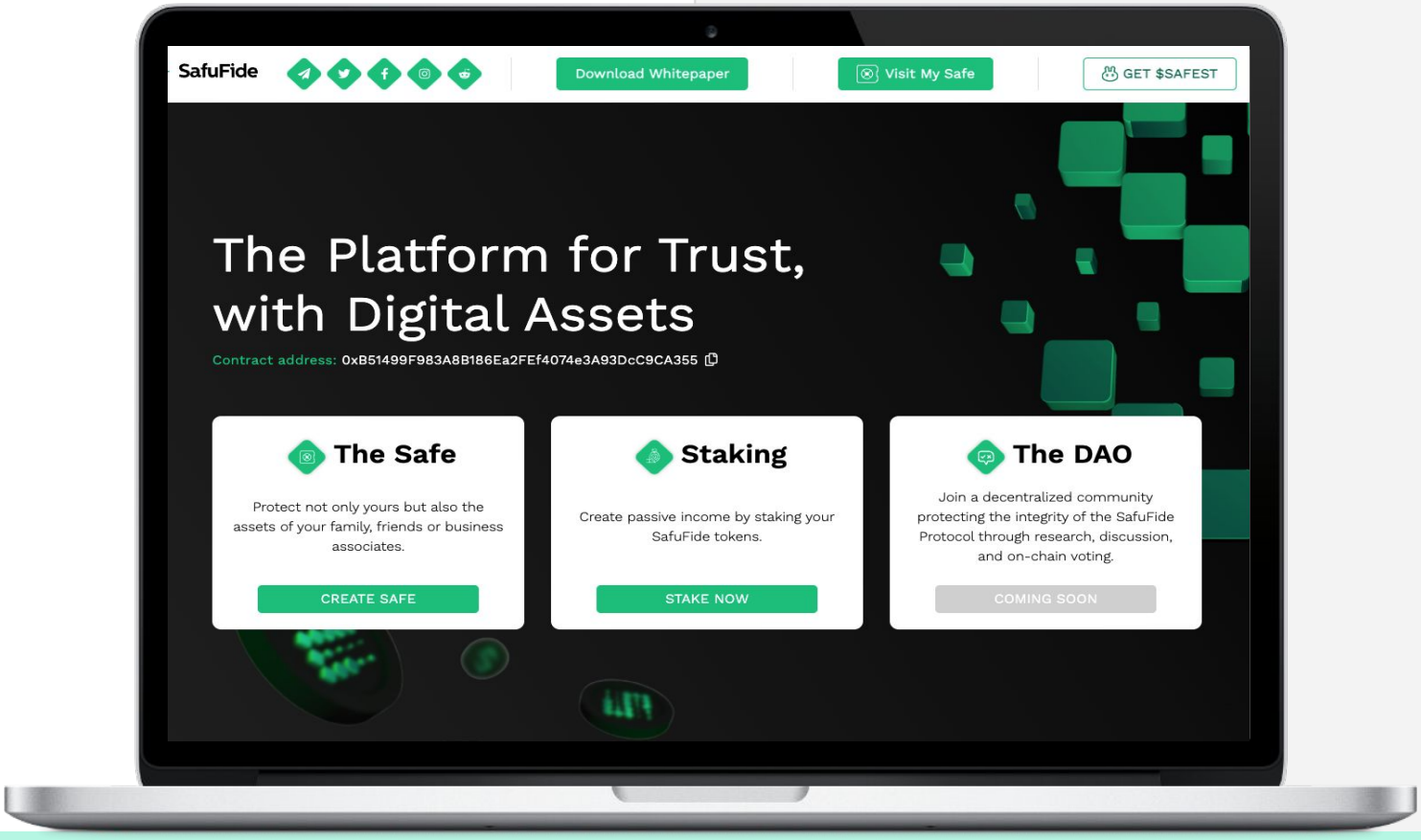
Design
No content available. ⚠️

Content
No content available. ⚠️

Whitepaper
No content available. ⚠️

Roadmap
No content available. ⚠️

Mobile-friendly?
Yes



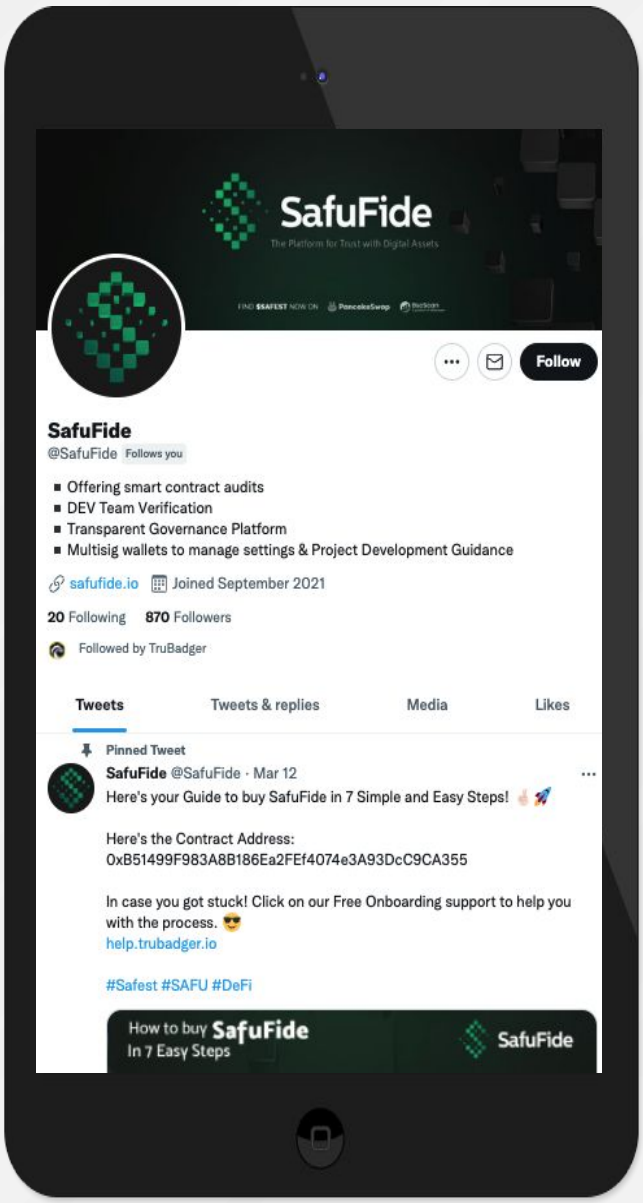
dogekart.io

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Social media accounts are relatively new and not very active.



Twitter

https://twitter.com/dogekart_racing

- 33 Followers
- Not active, 0 posts ⚠️

Discord

- Not available

Telegram

https://t.me/dogekart

- 16 members
- Few Active members
- Active mod

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.